

ABSTRAK

ANALISIS *VULNERABILITY MANAGEMENT* PADA *CONTAINER DOCKER* MENGUNAKAN *AQUASEC* DAN *ANCHORE* BERDASARKAN STANDAR *CYBER RESILIENCE REVIEW (CRR)*

Oleh

MILENIA ARI OKTAVIANA

NIM : 1202184238

Teknologi *container* yang banyak digunakan untuk menyediakan layanan IT salah satunya adalah Docker. Kerentanan pada teknologi *container* yaitu Docker membutuhkan pengelolaan secara khusus. Pengelolaan kerentanan ini dapat dilakukan secara teknis dengan *software vulnerability scanner* dan panduan standar *Cyber Resilience Review (CRR)*. Eksperimen dilakukan dengan *scanner* Aquasec dan Anchore yang melakukan *vulnerability scanning* pada dua sistem Docker Images. Dua sistem rentan tersebut memiliki perbedaan versi yaitu versi – 1 dan versi – 2. Elemen *software* pada versi – 2 memiliki tingkat *versioning* lebih tinggi daripada versi – 1. Data percobaan berupa *vulnerability report* dianalisis berdasarkan *Cyber Resilience Review (CRR)* yang berfokus pada empat tahap yaitu *Define a Strategy, Develop a Plan, Implement the Capability, Assess and Improve the Capability*. Sehingga didapatkan hasil *Category Vulnerability* yaitu 30 *Closed Vulnerability*, 10 *Open Vulnerability*, dan 13 *Newly Vulnerability*. Kelanjutan penelitian ini dapat menggunakan aspek *Patch Management* dengan *tools software* yang lebih bervariasi.

Kata Kunci: Docker, *Vulnerability*, *Scanner*, *Cyber Resilience Review (CRR)*